PGMLLL: 新しい多項式時間で停止する LLL with deep-insertions の提案
PGMLLL: A Development of A New Polynomial-time Variant of LLL with Deep-insertions

さとしん
立教大学大学院

2025 年 8 月 19 日

1 準備

1.1 記号の準備

本記事で使用する記号は以下の表に従う．

記号	意味
$\mathbb{Z}$	整数全体の集合
$\mathbb{Q}$	有理数全体の集合
$\mathbb{R}$	実数全体の集合
$\mathrm{M}_n(R)$	環 R 上の $n \times n$ 行列全体の集合
$\boldsymbol{O}_{n,m}$	$n \times m$ の零行列
$\boldsymbol{E}_n$	n 次単位行列
$q^{(\mathrm{num})}$, $q^{(\mathrm{den})}$	$q \in \mathbb{Q}$ の分子，及び分母（必ずしも**既約分数とは限らない**）
$\lfloor \bullet \rceil$	実数の四捨五入

2 格子

Definition 2.1 (格子)**.** 一次独立な n 本のベクトル $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^n$（これを**基底ベクトル**と呼ぶ）の整数係数の一次結合全体の集合

$$L = \mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) := \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \;\middle|\; a_1, \ldots . a_n \in \mathbb{Z} \right\}$$

を (完全階数な) **格子**と呼び，基底ベクトルの組 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を**基底**と呼ぶ．また，基底ベクトルが全て整数ベクトルであるとき，L を**整数格子**と呼び，本記事では整数格子のみ扱う．

2.1 Gram-Schmidt の直交化法

Definition 2.2 (Gram-Schmidt の直交化)**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とする．このとき

$$\begin{cases} \boldsymbol{b}_1^\star := \boldsymbol{b}_1, \\ \boldsymbol{b}_i^\star := \boldsymbol{b}_i - \displaystyle\sum_{j=1}^{i-1} \mu_{i,j}\boldsymbol{b}_j^\star,\ \mu_{i,j} := \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^\star \rangle}{\|\boldsymbol{b}_j^\star\|^2}\ (1 \leq j < i \leq n). \end{cases}$$

で定義される $\boldsymbol{b}_1^\star, \ldots, \boldsymbol{b}_n^\star$ を **Gram-Schmidt の直交化ベクトル**，$\boldsymbol{U} := (\mu_{i,j})_{i,j}$ を **Gram-Schmidt の直交化係数行列**と呼ぶ.

B1 や B2 の線形代数学で習うような Gram-Schmidt の直交化法そのものです.

2.2 体積

Definition 2.3 (体積)**.** L を n 次元格子として，$\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を L の基底とする．更に,

$$\boldsymbol{B} := \begin{bmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_n \end{bmatrix} \in \mathrm{M}_n(\mathbb{Z})$$

とする．このとき,

$$\mathrm{vol}(L) := \sqrt{\det(\boldsymbol{B}\boldsymbol{B}^\top)} = \prod_{i=1}^{n} \|\boldsymbol{b}_i^\star\|$$

を n 次元格子 L の**体積**または**行列式**と呼ぶ.

2.3 LLL

Definition 2.4 (LLL 簡約基底 (Lenstra, Lenstra and Lovász, 1982))**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とします．このとき，$\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ が簡約パラメタ $\frac{1}{4} < \delta < 1$ に対して **LLL 簡約されている**とは

$$\begin{array}{ll} (\textbf{サイズ簡約条件}) & 1 \leq {}^\forall j < {}^\forall i \leq n, \quad |\mu_{i,j}| \leq \frac{1}{2} \\ (\textbf{Lovász 条件}) & 2 \leq {}^\forall k < n, \qquad \delta\|\boldsymbol{b}_{k-1}^\star\| \leq \|\pi_{k-1}(\boldsymbol{b}_k)\|^2 \end{array}$$

を満たすときを言います.

Lovász 条件の不等式は

$$\|\boldsymbol{b}_k^\star\| \geq (\delta - \mu_{k,k-1}^2)\|\boldsymbol{b}_{k-1}^\star\|^2$$

と同値であるので，この不等式の方を Lovász 条件と呼ぶこともあります．LLL 簡約基底を求めるアルゴリズムは，多項式時間で停止することが知られています.

2.4 DeepLLL(LLL with deep-insertion)

DeepLLL 簡約は LLL 簡約の自然な一般化であり，以下の様に定義されます.

Definition 2.5 (DeepLLL 簡約基底 (Schnorr and Euchner, 1994))**.** $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とします．このとき，$\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ が簡約パラメタ $\frac{1}{4} < \delta < 1$ に対して **DeepLLL 簡約されている**とは

$$\begin{array}{ll} (\textbf{サイズ簡約条件}) & 1 \leq {}^{\forall}j < {}^{\forall}i \leq n, \quad |\mu_{i,j}| \leq \frac{1}{2} \\ (\textbf{deep-exchange 条件}) & 1 \leq {}^{\forall}i < {}^{\forall}k \leq n, \quad \delta \|\boldsymbol{b}_i^\star\| \leq \|\pi_i(\boldsymbol{b}_k)\|^2 \end{array}$$

を満たすときを言います．但し，写像

$$\begin{array}{rccl} \pi_\ell : & \mathbb{R}^n & \longrightarrow & \langle \boldsymbol{b}_1, \dots, \boldsymbol{b}_{\ell-1} \rangle_{\mathbb{R}}^{\perp} \quad = \langle \boldsymbol{b}_\ell^\star, \dots, \boldsymbol{b}_n^\star \rangle_{\mathbb{R}} \\ & \boldsymbol{x} & \longmapsto & \displaystyle\sum_{i=\ell}^{n} \frac{\langle \boldsymbol{x}, \boldsymbol{b}_i^\star \rangle}{\|\boldsymbol{b}_i^\star\|^2} \boldsymbol{b}_i^\star \end{array}$$

は $\mathbb{R}$ ベクトル空間 $\langle \boldsymbol{b}_1, \dots, \boldsymbol{b}_{\ell-1} \rangle_{\mathbb{R}}$ の直交補空間への直交射影とします．

Definition 2.6 (deep-insertion)**.** n 次元格子 L の基底 $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ に対して，**deep-insertion**$\sigma_{i,k}$ とは

$$\sigma_{i,k} : \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\} \longmapsto \{\dots, \boldsymbol{b}_{i-1}, \boldsymbol{b}_k, \boldsymbol{b}_i, \dots, \boldsymbol{b}_{k-1}, \boldsymbol{b}_{k+1}, \dots\}$$

で定義される写像である．

しかし，DeepLLL 基底を求めるアルゴリズムは LLL アルゴリズムとは異なり停止性は証明されておらず，潜在的には super-exponential な計算量をもつとされています (Gama and Nguyen, 2008)．また，deep-insertion 後の基底の Gram-Schmidt の直交化ベクトルについては次の定理が成立します．

Theorem 2.7 (Yamaguchi and Yasuda, 2018)**.** $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とし，さらに別の L の基底を

$$\{\boldsymbol{c}_1, \dots, \boldsymbol{c}_n\} \coloneqq \sigma_{i,k}(\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\})$$

とする．このとき，基底 $\{\boldsymbol{c}_1, \dots, \boldsymbol{c}_n\}$ の Gram-Schmidt の直交化情報 $(C_j)_{1 \leq j \leq n}$, $(\nu_{\ell,j})_{1 \leq \ell, j \leq n}$ は，$\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ の Gram-Schmidt の直交化情報 $(B_j)_j, (\mu_{\ell,j})$ 及び $D_\ell \coloneqq \|\pi_\ell(\boldsymbol{b}_k)\|^2$ を用いて次のように表すことができる．

$$C_j = \begin{cases} D_i & \text{if } j = i \\ \dfrac{D_j B_{j-1}}{D_{j-1}} & \text{if } i+1 \leq j \leq k \\ B_j & \text{else} \end{cases}$$

$$\nu_{\ell,j} = \begin{cases} \mu_{\ell-1,j-1} - \dfrac{\mu_{k,j-1}}{D_j} \displaystyle\sum_{h=j}^{\ell-1} \mu_{k,h} \mu_{\ell-1,h} B_h & \text{if } i+1 \leq j \leq k,\ j+1 \leq \ell \leq k \\ \mu_{\ell,j-1} - \dfrac{\mu_{k,j-1}}{D_j} \displaystyle\sum_{h=j}^{k} \mu_{k,h} \mu_{\ell,h} B_h & \text{if } i+1 \leq j \leq k,\ k+1 \leq \ell \leq n \\ \dfrac{1}{D_i} \displaystyle\sum_{h=i}^{\ell-1} \mu_{k,h} \mu_{\ell-1,h} B_h & \text{if } j = i,\ i+1 \leq \ell \leq k \\ \dfrac{1}{D_i} \displaystyle\sum_{h=i}^{k} \mu_{k,h} \mu_{\ell,h} B_h & \text{if } j = i,\ k+1 \leq \ell \leq n \\ \mu_{k,j} & \text{if } \ell = i,\ 1 \leq j \leq i-1 \\ \mu_{\ell-1,j} & \text{if } i+1 \leq \ell \leq k,\ 1 \leq j \leq i-1 \\ \mu_{\ell,j} & \text{else} \end{cases}$$

3 既存の多項式時間で停止する LLL with deep-insertions

3.1 PotLLL

PotLLL は Fontein, Schneider and Wagner, 2014 で初めて提案された LLL with deep-insertions の変種で，格子基底の potential と呼ばれる量 (定義 6) が Lovász 条件を満たさない 2 つの隣接する基底ベクトル $(\boldsymbol{b}_{k-1}, \boldsymbol{b}_k)$ を交換した際に単調減少することに着目し，基底の potential が単調に減少する deep-insertion のみを施すことにより多項式時間で停止する様に完了したものです.

Definition 3.1 (potential)**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とし，L_i を基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}$ で張られる i 次元格子とする．このとき,

$$\mathrm{Pot}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) \coloneqq \prod_{i=1}^{n} \mathrm{vol}(L_i)^2 = \prod_{i=1}^{n} \|\boldsymbol{b}_i^\star\|^{2(n-i+1)}$$

を基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の **potential** と呼ぶ.

また，PotLLL 簡約基底とは以下のような基底を言います.

Definition 3.2 (PotLLL 簡約基底 (Fontein, Schneider and Wagner, 2014))**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とする．このとき，$\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ が簡約パラメタ $\frac{1}{4} < \delta < 1$ **について PotLLL 簡約されている**，もしくは δ**-PotLLL 簡約されている**とは

$$\text{(サイズ簡約条件)} \quad \begin{array}{ll} \leq {}^\forall j < {}^\forall i \leq n, & |\mu_{i,j}| \leq \frac{1}{2} \\ 1 \leq {}^\forall i < {}^\forall k \leq n, & \delta \cdot \mathrm{Pot}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \leq \mathrm{Pot}(\sigma_{i,k}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\})) \end{array}$$

の 2 条件を満たすことを言う.

3.2 S²LLL

S²LLL は Yasuda and Yamaguchi, 2019 によって提案された多項式時間で停止する LLL with deep-insertion の変種で，PotLLL は potential を減少させていましたが，S²LLL は格子基底の **Gram-Schmdit の直交化ベクトルの二乗和**と呼ばれる量が Lovász 条件を満たさない 2 つの隣接する基底ベクトル $(\boldsymbol{b}_{k-1}, \boldsymbol{b}_k)$ を交換した際に単調減少することに着目し，基底の Gram-Schmdit の直交化ベクトルの二乗和が単調に減少する deep-insertion のみを施すことにより多項式時間で停止する様に改良したものです.

Definition 3.3 (Gram-Schmdit の直交化ベクトルの二乗和)**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とし，L_i を基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}$ で張られる i 次元格子とする．このとき,

$$\mathrm{SS}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) \coloneqq \sum_{i=1}^{n} \|\boldsymbol{b}_i^\star\|^2$$

を基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の **Gram-Schmdit の直交化ベクトルの二乗和**（**squared-sum of Gram-Schmdit lengths**）と呼ぶ.

Definition 3.4 (S²LLL 簡約基底 (Yasuda and Yamaguchi, 2019))**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とする．このとき，$\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ が簡約パラメタ $0 < \eta \leq 1$ **について S²LLL 簡約されている**，もしくは

η-S^{2}LLL 簡約されているとは

$$\text{(サイズ簡約条件)}\quad \begin{array}{ll} \leq {}^{\forall}j < {}^{\forall}i \leq n, & |\mu_{i,j}| \leq \frac{1}{2} \\ 1 \leq {}^{\forall}i < {}^{\forall}k \leq n, & \eta \cdot \mathrm{SS}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \leq \mathrm{SS}(\sigma_{i,k}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\})) \end{array}$$

の 2 条件を満たすことを言う.

4 新しく提案する簡約 PGMLLL

4.1 Gram-Schmidt 幾何平均の積

今回新しく LLL with deep-insertion の変種を提案するに当たって，新しい格子基底に対して定まる量を定義しました．具体的には，以下で定義されるものです.

Definition 4.1 (Gram-Schmidt 幾何平均の積)**.** $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とする．このとき,

$$\mathrm{GM}_k(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \coloneqq \left(\prod_{i=1}^{k} \|\boldsymbol{b}_i^\star\|^2\right)^{\frac{1}{k}} \quad (1 \leq k \leq n)$$

を格子基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の **Gram-Schmidt 幾何平均**（**Gram-Schmidt geometric mean**）と呼ぶことにし，その積

$$\begin{aligned} \mathrm{PGM}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) &\coloneqq \prod_{k=1}^{n} \mathrm{GM}_k(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \\ &= \prod_{k=1}^{n} \left(\prod_{i=1}^{k} \|\boldsymbol{b}_i^\star\|^2\right)^{\frac{1}{k}} \\ &= \prod_{i=1}^{n} \|\boldsymbol{b}_i^\star\|^{\sum_{k=i}^{n} \frac{2}{k}} \end{aligned}$$

を **Gram-Schmidt 幾何平均の積**（**potential of Gram-Schmidt geometric mean**）と呼ぶことにする.

4.2 Gram-Schmidt 幾何平均の積の性質

この，格子基底の Gram-Schmidt 幾何平均の積は，次の性質を持っています.

Proposition 4.2. $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を n 次元格子 L の基底とする．このとき, 隣り合う基底ベクトル $(\boldsymbol{b}_{k-1}, \boldsymbol{b}_k)$ が簡約パラメタ $\delta \in \left(\frac{1}{4}, 1\right)$ に関する Lovász 条件を満たさないとき，新しい L の基底を

$$\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n\} \coloneqq \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k-2}, \boldsymbol{b}_k, \boldsymbol{b}_{k-1}, \boldsymbol{b}_{k+1}, \ldots, \boldsymbol{b}_n\}$$

と定めると

$$\mathrm{PGM}(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n) < \delta^{\frac{1}{k-1}} \cdot \mathrm{PGM}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$$

が成立する.

Proof. 簡単のため，$B_i \coloneqq \|\boldsymbol{b}_i^\star\|^2, C_i \coloneqq \|\boldsymbol{c}_i^\star\|^2$ とします．このとき，$(\boldsymbol{b}_{k-1}, \boldsymbol{b}_k)$ が Lovász 条件を満たさない，即ち $B_k < (\delta - \mu_{k,k-1}^2) B_{k-1}$ であることから

$$C_{k-1} = B_k + \mu_{k,k-1}^2 B_{k-1} < \delta B_{k-1}$$

が成り立ちます．従って，

$$\begin{aligned}
\mathrm{PGM}(\boldsymbol{c}_1,\dots,\boldsymbol{c}_n) &= \prod_{j=1}^{n}\left(\prod_{i=1}^{j} C_i\right)^{\frac{1}{j}} \\
&= \prod_{j=1}^{k-2}\left(\prod_{i=1}^{j} B_i\right)^{\frac{1}{j}} \times \left(\prod_{i=1}^{k-1} C_i\right)^{\frac{1}{k-1}} \times \prod_{j=k}^{n}\left(\prod_{i=1}^{j} B_i\right)^{\frac{1}{j}} \\
&< \prod_{j=1}^{k-2}\left(\prod_{i=1}^{j} B_i\right)^{\frac{1}{j}} \times \left(\delta\prod_{i=1}^{k-1} B_i\right)^{\frac{1}{k-1}} \times \prod_{j=k}^{n}\left(\prod_{i=1}^{j} B_i\right)^{\frac{1}{j}} \\
&= \delta^{\frac{1}{k-1}} \prod_{j=1}^{n}\left(\prod_{i=1}^{j} B_i\right)^{\frac{1}{j}} \\
&= \delta^{\frac{1}{k-1}} \cdot \mathrm{PGM}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_n).
\end{aligned}$$

となります． □

Proposition 4.3. $\{\boldsymbol{b}_1,\dots,\boldsymbol{b}_n\}$ を n 次元格子 L の基底とし，$B_i \coloneqq \|\boldsymbol{b}_i^\star\|^2$ を Gram-Schmidt の直交化ベクトルの二乗ノルムとする．このとき，以下が成立する．

$$1 \le {}^\forall i < {}^\forall k \le n,\ \frac{\mathrm{PGM}(\sigma_{i,k}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_n))}{\mathrm{PGM}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_n)} = \prod_{j=i}^{k}\left(\frac{D_j}{B_j}\right)^{\frac{1}{j}}$$

ただし，$D_j \coloneqq \|\pi_j(\boldsymbol{b}_k)\|^2$ であり，写像

$$\begin{array}{rccl}
\pi_j\colon & \mathbb{R}^n & \longrightarrow & \langle \boldsymbol{b}_1,\dots,\boldsymbol{b}_{j-1}\rangle_{\mathbb{R}}^{\perp} = \langle \boldsymbol{b}_j^\star,\dots,\boldsymbol{b}_n^\star\rangle_{\mathbb{R}} \\
& \boldsymbol{x} & \longmapsto & \displaystyle\sum_{i=j}^{n} \frac{\langle \boldsymbol{x}, \boldsymbol{b}_i^\star\rangle}{\|\boldsymbol{b}_i^\star\|^2}\boldsymbol{b}_i^\star
\end{array}$$

は $\mathbb{R}$ ベクトル空間 $\langle \boldsymbol{b}_1,\dots,\boldsymbol{b}_{j-1}\rangle_{\mathbb{R}}$ の直交補空間への直交射影とする．

Proof. 定理 1 から以下が従います．

$$\begin{aligned}
&\frac{\mathrm{PGM}(\sigma_{i,k}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_n))}{\mathrm{PGM}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_n)} \\
=&\frac{\displaystyle\prod_{j=1}^{i-1}\left(\prod_{\ell=1}^{j} B_\ell\right)^{\frac{1}{j}} \times \left(D_i\prod_{\ell=1}^{i-1} B_\ell\right)^{\frac{1}{i}} \times \prod_{j=i+1}^{k}\left(D_j\prod_{\ell=1}^{j-1} B_\ell\right)^{\frac{1}{j}} \times \prod_{j=k+1}^{n}\left(D_k\prod_{\ell=1}^{k-1} B_\ell \cdot \prod_{\ell=k+1}^{j} B_\ell\right)^{\frac{1}{j}}}{\displaystyle\prod_{j=1}^{n}\left(\prod_{\ell=1}^{j} B_\ell\right)^{\frac{1}{j}}} \\
=&\frac{D_i^{\frac{1}{i}}}{B_i^{\frac{1}{i}}} \times \prod_{j=i+1}^{k}\frac{D_j^{\frac{1}{j}}}{B_j^{\frac{1}{j}}} \times \prod_{j=k+1}^{n}\frac{D_k^{\frac{1}{j}}}{B_k^{\frac{1}{j}}} \\
=&\prod_{j=i}^{k}\left(\frac{D_j}{B_j}\right)^{\frac{1}{j}} \times \left(\frac{D_k}{B_k}\right)^{\sum_{j=k+1}^{n}\frac{1}{j}} \\
=&\prod_{j=i}^{k}\left(\frac{D_j}{B_j}\right)^{\frac{1}{j}}. \quad \square
\end{aligned}$$

□

Corollary 4.4.

$$P_{i,k} \coloneqq \frac{\mathrm{PGM}(\sigma_{i,k}(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n))}{\mathrm{PGM}(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n)}$$

とする．このとき,

$$P_{i,k} = \left(\frac{\|\boldsymbol{b}_k\|^2 - \sum_{j=1}^{i-1}\mu_{k,j}^2 B_j}{B_i}\right)^{\frac{1}{i}} P_{i+1,k}$$

が成立する.

Proof.

$$\begin{aligned}
P_{i,k} &= \prod_{j=i}^{k}\left(\frac{D_j}{B_j}\right)^{\frac{1}{j}} \times \left(\frac{D_k}{B_k}\right)^{\sum_{j=k+1}^{n}\frac{1}{j}} \\
&= \left(\frac{D_i}{B_i}\right)^{\frac{1}{i}} \prod_{j=i+1}^{k}\left(\frac{D_j}{B_j}\right)^{\frac{1}{j}} \times \left(\frac{D_k}{B_k}\right)^{\sum_{j=k+1}^{n}\frac{1}{j}} \\
&= \left(\frac{D_i}{B_i}\right)^{\frac{1}{i}} P_{i+1,k}.
\end{aligned}$$

ここで,

$$D_i = \|\pi_i(\boldsymbol{b}_k)\|^2 = \|\boldsymbol{b}_k\|^2 - \sum_{j=1}^{i-1}\mu_{k,j}^2 B_j$$

を代入して

$$P_{i,k} = \left(\frac{\|\boldsymbol{b}_k\|^2 - \sum_{j=1}^{i-1}\mu_{k,j}^2 B_j}{B_i}\right)^{\frac{1}{i}} P_{i+1,k}$$

を得る. □

4.3 PGMLLL

この Gram-Schmidt 幾何平均の積とその性質（主に命題 2）を利用して PGMLLL 簡約基底を次のように定義します.

Definition 4.5. $\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}$ を n 次元格子 L の基底とします．このとき，$\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}$ が簡約パラメタ $\frac{1}{4} < \delta < 1$ に対して **PGMLLL 簡約されている**とは

$$\begin{aligned}
(\textbf{サイズ簡約条件}) \quad & 1 \le {}^{\forall}j < {}^{\forall}i \le n, \quad |\mu_{i,j}| \le \tfrac{1}{2} \\
& 1 \le {}^{\forall}i < {}^{\forall}k \le n, \quad \delta^{\frac{1}{i}} \cdot \mathrm{PGM}(\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}) \le \mathrm{PGM}(\sigma_{i,k}(\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}))
\end{aligned}$$

を満たすときを言う

.

4.4 PGMLLL アルゴリズム

Algorithm 1 に命題 3，並びにその系を利用した PGMLLL 簡約基底アルゴリズムを示す.

Algorithm 1 PGMLLL(δ) : 簡約パラメタδに関する PGMLLL 基底簡約アルゴリズム
Input : n 次元格子の基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
Output : δに関する PGMLLL 簡約基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
$(B_i)_{1\leq i\leq n}, (\mu_{i,j})_{1\leq i,j\leq n} \leftarrow$ `gram_schmidt`()
$k \leftarrow 1$
while $k \leq n$ **do**
  for $j = k-1$ downto 1 **do**
    `size_reduce`(k, j)
  $P \leftarrow 1;\ P_{\min} \leftarrow 1$
  $i \leftarrow 1$
  for $j = k-1$ downto 1 **do**
    $P \leftarrow P \cdot \left(\frac{B_k + \sum_{\ell=j}^{k-1} \mu_{k,\ell}^2 B_\ell}{B_j}\right)^{\frac{1}{j}}$
    if $P < P_{\min}$ **then**
      $i \leftarrow j$
      $P_{\min} \leftarrow P$
  if $\delta^{\frac{1}{i}} > P_{\min}$ **then**
    $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \leftarrow \sigma_{i,k}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\})$
    Gram-Schmidt の直交化情報の更新
    $k \leftarrow i$
  else
    $k \leftarrow k+1$

但し，`gram_schmidt`() は基底の Gram-Schmidt の直交化ベクトルの二乗ノルムと Gram-Schmidt の直交化係数行列（この 2 つをまとめて **Gram-Schmidt の直交化情報**と呼ぶことにする）を計算する関数，`size_reduce`(k, j) はサイズ基底簡約アルゴリズム，`updata_gso_deep_insertion`(i, k) は deep-insertion$\sigma_{i,k}$ を施した後の Gram-Schmidt の直交化情報の更新アルゴリズムで，それぞれ以下のアルゴリズムの様になる.

Algorithm 2 gram_schmidt() : Gram-Schmidt の直交化情報を求める
Input : n 次元格子の基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
Output : $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の Gram-Schmidt 情報 $(B_i)_i$, $(\mu_{i,j})_{i,j}$
$B \leftarrow \boldsymbol{0}_n$
$\mu \leftarrow \boldsymbol{E}_n$
$\boldsymbol{b}_1^\star \leftarrow \boldsymbol{0}_n;\ \cdots;\ \boldsymbol{b}_n^\star \leftarrow \boldsymbol{0}_n$
for $i = 1$ to n **do**
  $\boldsymbol{b}_i^\star \leftarrow \boldsymbol{b}_i$
  for $j = 1$ to $i-1$ **do**
    $\mu_{i,j} \leftarrow \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^\star \rangle}{B_j}$
    $\boldsymbol{b}_i^\star \leftarrow \boldsymbol{b}_i^\star - \mu_{i,j}\boldsymbol{b}_j^\star$
  $B_i \leftarrow \|\boldsymbol{b}_i^\star\|^2$
return B, μ

Algorithm 3 size_reduce(i, j) : 部分的なサイズ基底簡約
Input： n 次元格子の基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$，その Gram-Schmidt の直交化係数行列 $(\mu_{i,j})_{i,j}$
Output： 簡約された基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ と更新された Gram-Schmidt の直交化係数行列 $(\mu_{i,j})_{i,j}$
1 **if** $|\mu_{i,j}| > \frac{1}{2}$ **then**
2 $\quad q \leftarrow \lfloor \mu_{i,j} \rceil$
3 $\quad \boldsymbol{b}_i \leftarrow \boldsymbol{b}_i - q\boldsymbol{b}_j$
4 $\quad$ **for** $\ell = 1$ to j **do**
5 $\quad\quad \mu_{i,\ell} \leftarrow \mu_{i,\ell} - q\mu_{j,\ell}$

4.5 PGMLLL の計算量

まず，PGMLLL における 3 行目から始まる **while** 文の呼び出し回数について次がわかります．

Proposition 4.6. Algorithm 1 に基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を入力したとして，$X \coloneqq \max\{\|\boldsymbol{b}_1\|^2, \ldots, \|\boldsymbol{b}_n\|^2\}$ とする．このとき，Algorithm 1 で deep-insertion が行われる回数は高々 $\mathcal{O}(n^2 \log X)$ である．

Proof. Algorithm 1 の 14 行目の deep-insertion の呼び出し回数を N とします．Algorithm 1 より，呼び出される各 deep-insertion$\sigma_{i,k}$ により，格子基底の Gram-Schmidt の幾何平均の積を $\delta^{\frac{1}{i}}$ 倍ずつ減少させていきます．$\frac{1}{4} < \delta < 1$ であるから

$$\frac{1}{4} < \delta < \delta^{\frac{1}{2}} < \delta^{\frac{1}{3}} < \cdots < \delta^{\frac{1}{n}} < 1$$

が成立します．従って，格子基底の Gram-Schmidt の幾何平均の積は各 deep-insertion 毎に少なくとも $\delta^{\frac{1}{n}}$ ずつ減少します．他方で，Gram-Schmidt の幾何平均の積の定義から

$$\begin{aligned}
\mathrm{PGM}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) &= \prod_{k=1}^{n} \mathrm{GM}_k(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \\
&= \prod_{k=1}^{n} \left(\prod_{i=1}^{k} \|\boldsymbol{b}_i^\star\|^2 \right)^{\frac{1}{k}} \\
&= \prod_{k=1}^{n} \mathrm{vol}(L_i)^{\frac{1}{k}} \geq 1
\end{aligned}$$

であることがわかります．従って，

$$\delta^{\frac{N}{n}} \mathrm{PGM}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \geq 1$$

です．よって，

$$\begin{aligned}
&\delta^{\frac{N}{n}} \mathrm{PGM}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}) \geq 1 \\
\iff &\frac{N}{n} + \log_\delta [\mathrm{PGM}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\})] \leq 0 \\
\iff &N \leq -n \log_\delta [\mathrm{PGM}(\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\})]
\end{aligned}$$

となります．ここで，

$$\begin{aligned}\mathrm{PGM}(\{\boldsymbol{b}_1,\dots,\boldsymbol{b}_n\}) &= \prod_{k=1}^{n}\left(\prod_{i=1}^{k}\|\boldsymbol{b}_i^\star\|^2\right)^{\frac{1}{k}}\\ &\le \prod_{k=1}^{n}\left(\prod_{i=1}^{k}\|\boldsymbol{b}_i\|^2\right)^{\frac{1}{k}}\\ &\le \prod_{k=1}^{n}\left(X^k\right)^{\frac{1}{k}} = X^n\end{aligned}$$

ですので，前の式と合わせて

$$\begin{aligned}N &\le -n\log_\delta\left[\mathrm{PGM}(\{\boldsymbol{b}_1,\dots,\boldsymbol{b}_n\})\right]\\ &= n\log_{\frac{1}{\delta}}\left[\mathrm{PGM}(\{\boldsymbol{b}_1,\dots,\boldsymbol{b}_n\})\right]\\ &\le n\log_{\frac{1}{\delta}} X^n\end{aligned}$$

となります．従って，総回数 N は高々 $\mathcal{O}(n^2\log X)$ です． □

5 PGMLLL の実装 and 実験

今回は `SageMath` ではなく，`C++` で `NTL` ライブラリを用いて実装しました．実際のコードはを見ていただくか，本記事の末尾をご覧ください．

5.1 PGM の挙動

まず，80 次元における SVP Challenge の seed0 の基底に関して PGM の挙動をプロットしました．それが以下の図たちです．

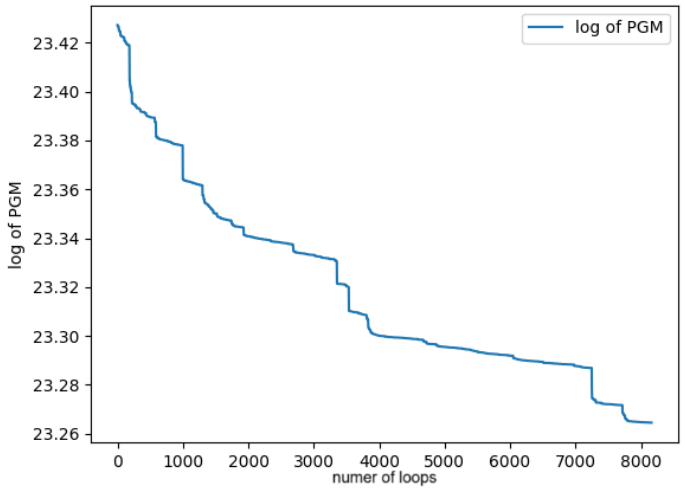

図 1 80 次元における log PGM の挙動

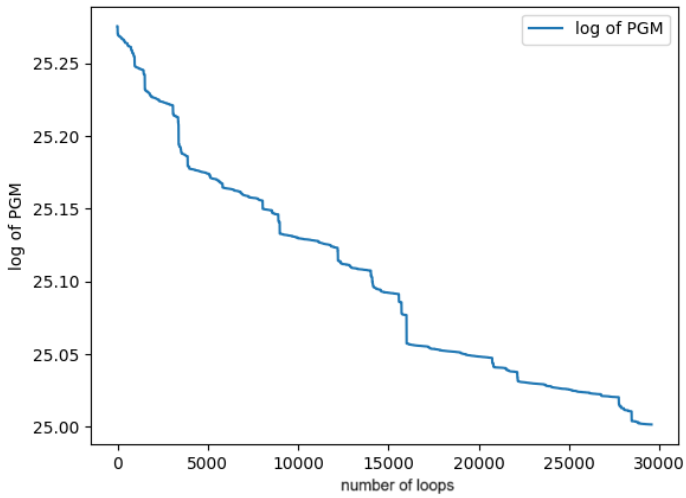

図 2　100 次元における log PGM の挙動

5.2　RHF の比較

まず，格子基底の RHF とは次のように定義されるものです．

Definition 5.1 (Root of Hermite factor(RHF))**.** 格子基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の **root of Hermite factor** もしくは **RHF** とは

$$\mathrm{rhf}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) \coloneqq \sqrt[n]{\frac{\|\boldsymbol{b}_1\|}{\sqrt[n]{\mathrm{vol}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)}}}$$

である．

SVP Challenge の seed0，40 次元〜150 次元までの基底に関して簡約パラメタ $\delta = 0.99$ での LLL，PGMLLL，そしてブロックサイズ $\beta = 10, 15$ での BKZ を施し，RHF をプロットしました．ただし，LLL は `SageMath` の `LLL` 関数を BKZ は `NTL` ライブラリの `BKZ_FP` 関数を利用しました．

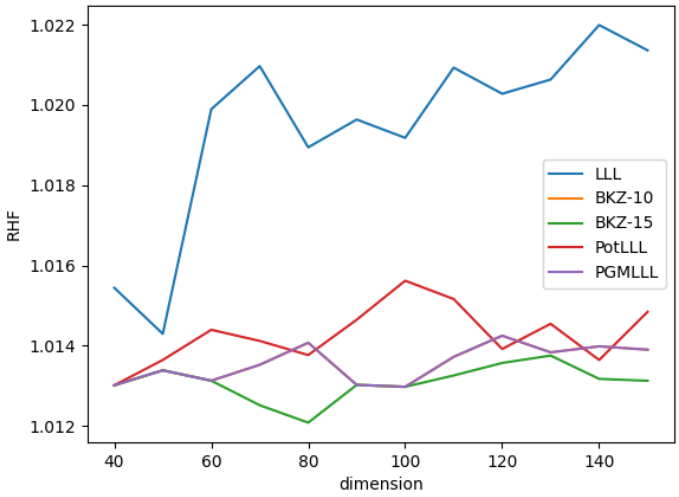

図 3　RHF の比較

図 4 から，少なくとも 150 次元程度まででは，ブロックサイズ $\beta = 10$ の BKZ と同じ品質であり，ブロックサイズ $\beta = 15$ の BKZ とほぼ同程度の品質を維持することがわかります．